DATE(S) ISSUED:

4/28/2014

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 6 through Internet Explorer 11.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 6

- Microsoft Internet Explorer 7

- Microsoft Internet Explorer 8

- Microsoft Internet Explorer 9

- Microsoft Internet Explorer 10

- Microsoft Internet Explorer 11

RISK:

Government:

- Large and medium government entities: **High**

- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been reported affecting all versions of Internet Explorer that could allow for remote code execution. This vulnerability exists due to the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code, in the context of the current user, within Internet Explorer. An attacker could host a specially crafted website designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.
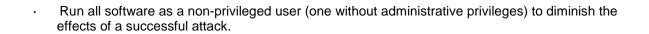
Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 6 and Internet Explorer 11.

RECOMMENDATIONS:

The following actions should be taken:

- Consider using an alternate browser until a patch is made available for the vulnerable versions of Internet Explorer.
- Consider implementing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) as it has been reported to make the vulnerability difficult to exploit.
- Run Internet Explorer with Protected Mode enabled
- Set Internet and Local intranet security zone settings to "High"
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Fireeye:

http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html

Microsoft:

https://technet.microsoft.com/en-US/library/security/2963983

http://technet.microsoft.com/en-US/security/jj653751

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776